



Ruhr Master School
of Applied Sciences

Dieses Wahlpflichtmodul ist ein Angebot der:

**Fachhochschule
Dortmund**

University of Applied Sciences and Arts

**Masterstudiengang
Energiesysteme**

IT-Sicherheit

sekretariat.fb3@fh-dortmund.de
0231 9112-9207 /-9283

Prof. Dr. Michael Berger
michael.berger@fh-dortmund.de

Hochschule Bochum
Bochum University
of Applied Sciences



**Fachhochschule
Dortmund**
University of Applied Sciences and Arts



**Westfälische
Hochschule**
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

**STIFTUNG
MERCATOR**



IT-Sicherheit					
Kürzel ITS	Workload in h 240	Credits 8	Fachsemester 1, 2 oder 3	Häufigkeit Sommersem.	Dauer 1 Semester
1	Lehrveranstaltungen			Kontaktzeit in h	Selbststudium in h
	IT-Sicherheit in Energienetzen			36	84
	Robuste Datensysteme			36	84
2	Lernergebnisse (learning outcomes)/Kompetenzen				
	Die Studierenden haben Detailkenntnisse über die Anforderungen und Ausführungen von sicheren IT-Systemen und robusten Datensystemen für die Steuerung und Überwachung von kritischen Infrastrukturen. Sie kennen insbesondere die gesetzlichen Anforderungen des IT-Sicherheitsgesetzes, BSI-Gesetzes, BSI-Kritis-Verordnungen, IT-Sicherheitskataloges (EnWG §11Abs. 1a) und (EnWG §11Abs. 1b) sowie die Ausführungshinweise der Normen DIN ISO/IEC 27001, DIN ISO/IEC 27002 und DIN ISO/IEC TR 27019 für die Assets des Geltungsbereiches, wie z. B. Steuerungs- und Telekommunikationssysteme, IT-Bestandssysteme, wie EDM-, GIS-, Marktkommunikations- und Prozessleit-Systeme. Es können die notwendigen technischen wie auch organisatorischen Maßnahmen zum sicheren Betrieb der kritischen Infrastruktur abgeleitet sowie eine umfassende Risikoanalyse, -bewertung und -behandlung erstellt werden. Hierzu gehören Maßnahme zur Datensicherung, Testverfahren, hardware- als auch softwareseitige Systemhärtung sowie auch der Einsatz von kryptografischer Verfahren. Neben den Fachkenntnissen haben die Studierenden in diesem Modul auch Schlüsselqualifikationen erlangt.				
3	Inhalte				
	IT-(Informationssicherheit)-Sicherheit in Energienetzen: - Bedrohungslage und Gefährdungspotenziale kritischer Infrastrukturen, insbesondere Energienetze (ÜBN, VNB) (weitere Betrachtung um den intelligenten Messstellenbetreiber (iMSB) und Energieanlagen) - gesetzte Anforderungen (IT-Sicherheitsgesetz, BSI-Gesetz, BSI-Kritis-Verordnungen, IT-Sicherheitskatalog (EnWG §11Abs. 1a), IT-Sicherheitskatalog (EnWG §11Abs. 1b), BSI Technische Richtlinie (TR-03109)) - kritische Geschäftsprozesse und deren Modellierung (Notation: EPK, BPMN2.0, ...) - Normen (DIN ISO/IEC 27001, DIN ISO/IEC 27002, DIN ISO/IEC TR 27019) - Managementsystem (Informationssicherheit und Datenschutz) - Risikomanagement (Schutzbedarf, Assets, Bedrohung, Schwachstellen, Schadenskategorien nach dem IT-Sicherheitskatalog der BNetzA (Bundennetzagentur)) Robuste Datensysteme: - Maßnahme aus der DIN ISO/IEC 27001 und DIN ISO/IEC TR 27019 - Grundlagen der digitalen Forensik - Grundlagen diskreter Mathematik und Zahlentheorie - Grundlagen der Kryptologie (Symmetrische und asymmetrische Chiffren) - Verfahren zum Schutz der Vertraulichkeit, Integrität und Authentizität (Verschlüsselungen, Hashen, Signieren...) - Verfahren zum Schutz der Verfügbarkeit (Sicherung- und Wiederherstellung /Disaster Recovery, ...) - Business Continuity und IT-Notfallmanagement - Wartungsprozesse und -konzepte: Patch- und Updatefähigkeit, Systemredundanz, Test und Rollout und Wiederherstellungsstrategien - Zugangs- und Zugriffsrechte (Benutzerrollen und -authentifizierung, Passwort-Policy, ...) - Zonenkonzepte - IT-Architekturen				

4	<u>Lehrformen</u> Seminaristische Veranstaltung, Praktische Durchführung des Aufbaus und des Tests eines sicheren und robusten Datensystems zur Steuerung und Überwachung von Energienetzen.
5	<u>Teilnahmevoraussetzungen</u> Formal gelten die Vorgaben der jeweils gültigen Prüfungsordnung Inhaltlich:
6	<u>Prüfungsformen</u> Klausur oder mündliche Prüfung (je nach Teilnehmerzahl und in Absprache mit dem ganzen Kurs)
7	<u>Voraussetzungen für die Vergabe von Kreditpunkten</u> Modulprüfung muss bestanden sein
8	<u>Verwendung des Moduls</u> MA Energiesysteme
9	<u>Stellenwert der Note für die Endnote</u> 5,33%
10	<u>Modulbeauftragte/r und hauptamtlich Lehrende/r</u> Modulbeauftragte/r: Prof. Dr. Michael Berger hauptamtlich Lehrende/r: Prof. Dr. Michael Berger
11	<u>Literatur</u> Appelrath, H, u.a. 2012. IT-Architekturentwicklung im Smart Grid. bitkom und VKU. 2015. Praxisleitfaden IT-Sicherheits-katalog. BDEW: Whitepaper- Anforderungen an sichere Steuerungs- und Telekommunikationssysteme BDEW: Ausführungshinweise zur Anwendung des Whitepaper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme BDEW: Checkliste zum Whitepaper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme BSI: Technische Richtlinie TR-03109, TR-03109-1 bis TR-03109-6 sowie Testspezifikationen (TS) BSI (Bundesamt für Sicherheit in der Informationstechnik). 2015. KRITIS-Sektorstudie – Energie. Klipper, S. 2015. Information Security Risk Management. Springer Verlag. FNN/DVGW. 2015. Informationssicherheit in der Energiewirtschaft. VDE. 2014. Positionspapier Smart Grid Security Energieinformationsnetze und –systeme. Kävrestad, J. 2018. Fundamentals of Digital Forensics Theory, Methods, and Real-Life Applications. Berlin. Springer-Verlag. Kersten, H. und G. Klett. 2017. Business Continuity und IT-Notfallmanagement. Grundlagen, Methoden und Konzepte. Springer Verlag. Witte, F. 2016. Testmanagement und Softwaretest. Theoretische Grundlagen und praktische Umsetzung. Springer Verlag Paar und Pelzl. 2016. Kryptografie verständlich Ein Lehrbuch für Studierende und Anwender. Berlin: Springer-Verlag. Eckert, C.: IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg
12	<u>Anmerkung</u> -